Exam

Key

True/False

1) [4] (§0 #7) If a and b are positive integers, then $a \cdot b = \text{lcm}(a,b)\,\gcd(a,b)$

start .5

True (+1)

Let $p_1, p_2, \ldots p_n$ be the prime divisors of a & b so that $a = p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n}$ and $b = p_1^{s_1} p_2^{s_2} \cdots p_n^{s_n}$ where r_i and s_i are elements of $\mathbb{Z}_{\geq 0}$

Recall $\gcd(a,b) = p_1^{\min(r_1,s_1)} p_2^{\min(r_2,s_2)} \cdots p_n^{\min(r_n,s_n)}$

and $\text{lcm}(a,b) = p_1^{\max(r_1,s_1)} p_2^{\max(r_2,s_2)} \cdots p_n^{\max(r_n,s_n)}$.

Then

$$a \cdot b = (p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n})(p_1^{s_1} p_2^{s_2} \cdots p_n^{s_n}) = p_1^{r_1+s_1} p_2^{r_2+s_2} \cdots p_n^{r_n+s_n}$$

and

$$\text{lcm}(a,b) \cdot \gcd(a,b) = \left[p_1^{\min(r_1,s_1)} \cdots p_n^{\min(r_n,s_n)}\right] \cdot \left[p_1^{\max(r_1,s_1)} \cdots p_n^{\max(r_n,s_n)}\right]$$

$$= p_1^{\min(r_1,s_1)+\max(r_1,s_1)} \cdots p_n^{\min(r_n,s_n)+\max(r_n,s_n)}$$

$$= p_1^{r_1+s_1} p_2^{r_2+s_2} \cdots p_n^{r_n+s_n}$$

So they are equal ☺

2) [4] (§1 #11) Let a, b, c be elements of the group D_4. If $ab = bc$ then $a = c$.

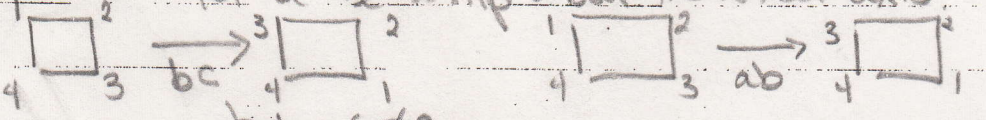
start +.5

False. (+1)

Let b be rotation counterclockwise by 90°

Let c be a flip about the horizontal axis &

Let a be a flip about the vertical axis.



$b \neq c$ $c \neq a$

3) [4] (§3) Let G be a group & H a subset of G. H is closed under the group operation. Then H is a subgroup of G.

start +.5

False (+1)

Let $G = \mathbb{Z}$ under addition

Let $H = \{x \in \mathbb{Z} \mid x \geq 0\}$ note H is closed

but H is not a subgroup (no inverses)

start +.5

4) [4] (§2) If $(ab)^2 = a^2 b^2$ in a group G, then G is abelian.

False (+1)

Aug ☹ I meant to write "for all a, b in G", grumble

Consider D_4, let a be a vertical flip & b a horz flip.

5. [9] (§2) For each of the sets and operations below, fill in the entries with yes or no. If no, briefly explain why. If yes, briefly describe the process you used to reach that anwer.

Sets S & Operator $\star$	Forms a Group	Abelian Group
a) $\{e, a, b, c\}$ $\star$ | e a b c e | e a b c a | a e c b b | b c e a c | c b a e start +5 reason +1 sense +5	yes +5 no extra/surprise elements show up $\Rightarrow$ closure there is an identity (e) each element has an inverse	yes +5 b/c the Cayley table is symmetric about the main diagonal
b) $\mathbb{Z}_8$ $\star$ standard multiplication start +5 reason +1 sense +5	no +5 $\mathbb{Z}_8$ is not closed under normal multiplication	if +5 this is not a group it certainly can't be abelian
c) $\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle\| ad - bc \neq 0 \& a, b, c, d \in \mathbb{R} \right\}$ $\star$ is matrix multiplication start +5 reason +1 sense +5	yes +5 its the general linear group of 2x2 matrices? Certainly closed b/c mult will return 2x2 matrix B/c the determinant isn't zero	No, +5 matrix multiplication is not commutative i.e $A \cdot B$ may not equal $B \cdot A$

4.75

Free Response: Show your work for the following problems. The correct answer with no supporting work will receive NO credit.
(If you use a calculator, be sure to tell me.)

6. [3] Describe one application in the world that makes use of one of the mathematical structures discussed thus far in class.

+.5 start
application +1
relating to the class +.5

Lots of examples exist in §0 and the readings that you've been reading/working/tracks for?
check digits on credit cards, magic card tricks, descriptory chemistry etc.

7. [8] (§3) Let G be a finite group and consider the Cayley table for G. (i.e. the table that shows all possible pairs of binary operators of G). Show that every element of G occurs precisely once in each row of the table.

start +.5
understanding +.5
logic +4
+2 each way
sense/notation +1.5
intro/writing +1.5

We first show that no duplicates appear then we use the pigeonhole principal to show all elements of G occure precisely once.
Assume towards contradiction that an element $g \in G$ appears twice in one row of the Cayley table. Then that means $\exists\, a,b,c \in G$ such that $ab=g$ and $ac=g$. Since G is a group $\exists! a^{-1} \in G$ $\Rightarrow b=a^{-1}g$ and $c=a^{-1}g \Rightarrow c=b$. Thus g can appear at most once.
Since there are $|G|$ elements in the row, each element can appear no more than once all elements must appear to fill in the entire row.

8. Consider the set $S = \{1, 2, 3, \ldots n-2, n-1\}$ where n is a positive integer.

(a) [2] (§2 #35) When does S form a group under multiplication?

start +.5
something that +.5
+1

"under" I meant to write "under multiplication modulo n"

as written:
when $S=\{1\}$ (i.e. $n=2$)

as I meant to write
when n is prime.

start +.5
something that +.5
+1

(b) [6] (§2 & 0) Prove your assertion.

start +.5

as written:
+1.5 Certainly when $S=\{1\}$ S forms a group where 1 is the identity.
sense/notation +.5
intro/writing +.5
+2 If $n>2$ then consider the element $n-1>1$.
Notice $(n-1)(n-1) > n-1$
thus $(n-1)^2$ is not in S and S is not closed
true +1

as I meant to write:
start +.5
If n is prime, S is a group b/c
+1.5 Associativity: is inherited from multiplication
Closure: modulo n guarantees we have closure
Identity: 1 acts as the identity
Inverses: Notice if n is prime, $\forall x \in S$
sense/notation +1
writing +1
+2 $\gcd(x,n)=1$ so $\exists\, s,t \in \mathbb{Z}$
$\Rightarrow xs+tn=1 \Rightarrow xs=1 \bmod n$
So $x^{-1}=s$, i.e we have inverses?
If S is a group then n is prime b/c
$\forall x \in \mathbb{Z} \Rightarrow 0<x<n$ $\exists\, s \in \mathbb{Z} \Rightarrow$
$xs=1 \bmod n \Rightarrow \gcd(x,n)=1$.

9. (§4) Let $G = \mathbb{Z}_{60}$ under addition modulo 60.

(a) [2] Find $|G|$. 60

(b) [3] Calculate the order of the element 49 in G.

$o(49) = \frac{60}{\gcd(49,60)} = \frac{60}{1} = 60$ (+1) by a theorem from §4 (+1)

49 = 7 · 7

60 = 6 · 10 = (2 · 3) · (2 · 5)

Know what order is (+1)

(c) [3] List four elements of order 15 in G.

We need to find x s.t. $\frac{60}{\gcd(x,60)} = 15$ (+1)

$\Rightarrow 60 = 15 \gcd(x,60)$ $\Rightarrow \gcd(x,60) = 4$ (+1.5)

So 4, 8, 16, 24

(+1.5) (+1.5) (+1.5)

(d) [2] Find a subgroup of G that has order 5.

$\langle 12 \rangle = \{12, 24, 36, 48, 0\}$

(e) [6] Write down the subgroup lattice for $\mathbb{Z}_{60}$

(+1.5) note: 60 = 6 · 10 = (2 · 3) · (2 · 5)

(+1) $\Rightarrow$ the subgroups are:

$\langle 2 \rangle, \langle 3 \rangle, \langle 4 \rangle, \langle 5 \rangle, \langle 6 \rangle, \langle 10 \rangle, \langle 12 \rangle, \langle 15 \rangle, \langle 20 \rangle, \langle 30 \rangle, \langle 0 \rangle$

organization (+1.5) from each step $\Rightarrow$ (4.5)